PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-143889
(43)Date of publication of application : 20.05.2004

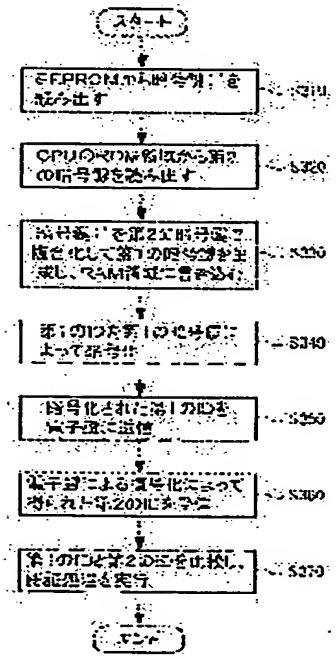
(51)Int.Cl. E05B 49/00
B60R 25/00
B60R 25/10
G06K 17/00
H04L 9/08
H04L 9/32

(21)Application number : 2002-312807
(22)Date of filing : 28.10.2002

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : IKEDA KAZUYA

(54) IN-VEHICLE INSIDE ELECTRONIC KEY DEVICE AND AUTHENTICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an in-vehicle electronic key device by making it difficult to forget an electronic key by acquiring a cipher key from an in-vehicle device, and to provide an authentication method.
SOLUTION: The in-vehicle electronic key device is provided with a step S310 for reading the cipher key to be ciphered obtained to cipher a first cipher key from a non-volatile memory; a step S320 for reading a second cipher key for decoding the cipher key to be ciphered and first discrimination information from an ROM region; a step S330 for storing to generate the first cipher key by using the second cipher key; a step S340 for ciphering the first discrimination information by using the first cipher key stored in an RAM region; a step S350 for transmitting the first ciphered discrimination information to an outside communication device; a step S360 for receiving a signal including second discrimination information stored by the outside communication device; and a step S370 for processing authentication by using the second discrimination information included in a received signal and the first discrimination information.



LEGAL STATUS

[Date of request for examination] 29.09.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-143889
(P2004-143889A)
(43)公開日　平成16年5月20日(2004.5.20)

(51)Int.Cl.[7]	F I		テーマコード（参考）
E05B 49/00	E05B 49/00	K	2E250
B60R 25/00	B60R 25/00	606	5B058
B60R 25/10	B60R 25/10	617	5J104
G06K 17/00	G06K 17/00	T	
H04L 9/08	H04L 9/00	601A	

審査請求 未請求　請求項の数 4　OL　（全 8 頁）　最終頁に続く

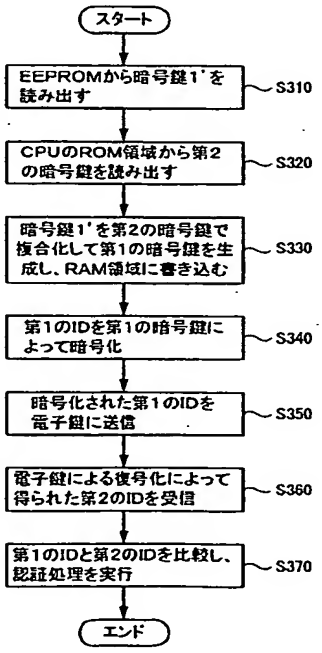
(21)出願番号　特願2002-312807(P2002-312807)
(22)出願日　平成14年10月28日(2002.10.28)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100072604
弁理士　有我　軍一郎
(72)発明者　池田　和也
神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内

Fターム(参考)　2E250 AA21 BB08 CC15 DD06 EE09 FF27 FF36 HH01 JJ05 KK03 LL01 TT03
5B058 CA17 KA02 KA04 KA08 KA31 KA35 YA11
5J104 AA07 KA02 KA04 KA06 KA15 NA37 NA38 PA15

(54)【発明の名称】車載電子鍵装置および認証方法

(57)【要約】
【課題】車載装置から暗号鍵を取得して電子鍵を偽造することを困難にするための車載電子鍵装置および認証方法を提供すること。
【解決手段】第１の暗号鍵を暗号化して得られる被暗号化暗号鍵を不揮発性メモリから読み出すステップＳ３１０と、被暗号化暗号鍵を復号化するために用いる第２の暗号鍵および第１の識別情報をＲＯＭ領域から読み出すステップＳ３２０と、第２の暗号鍵を用いて第１の暗号鍵を生成して記憶するステップＳ３３０と、ＲＡＭ領域に記憶された第１の暗号鍵を用いて第１の識別情報を暗号化するステップＳ３４０と、暗号化した第１の識別情報を外部の通信装置に送信するステップＳ３５０と、外部の通信装置が記憶する第２の識別情報を含む信号を受信するステップＳ３６０と、受信した信号中に含まれる第２の識別情報と第１の識別情報とを用いて認証処理を行するステップＳ３７０と、を備えた構成を有している。
【選択図】　図３



【特許請求の範囲】
【請求項１】
第１の暗号鍵を暗号化して得られる被暗号化暗号鍵を記憶する不揮発性メモリと、前記不揮発性メモリが記憶する前記被暗号化暗号鍵を復号化して前記第１の暗号鍵を生成するために用いる第２の暗号鍵をＲＯＭ領域に記憶した演算処理部とを備え、作動が停止しても前記第２の暗号鍵の情報を保持する記憶領域であることを特徴とする車載電子鍵装置。
【請求項２】
外部の通信装置と無線通信するための無線通信インタフェースを備え、前記演算処理部は、さらに認証処理に用いる第１の識別情報をＲＯＭ領域に記憶し、作動時または作動後に前記第２の暗号鍵を用いて前記被暗号化暗号鍵を復号化して前記第１の暗号鍵を生成し、生成した前記第１の暗号鍵をＲＡＭ領域に記憶し、前記ＲＡＭ領域に記憶された第１の暗号鍵を用いて前記第１の識別情報を暗号化し、前記暗号化した前記第１の識別情報を前記無線通信インタフェース経由で前記外部の通信装置に送信し、前記外部の通信装置が記憶する第２の識別情報を含む信号を前記無線通信インタフェース経由で受信し、受信した前記信号中に含まれる前記第２の識別情報と前記第１の識別情報とを用いて認証処理を行い、前記ＲＯＭ領域に記憶された前記第１の識別情報は、作動が停止しても情報が保持されることを特徴とする請求項１記載の車載電子鍵装置。
【請求項３】
第１の暗号鍵を暗号化して得られる被暗号化暗号鍵を不揮発性メモリから読み出すステップと、前記被暗号化暗号鍵を復号化するために用いる第２の暗号鍵および第１の識別情報をＲＯＭ領域から読み出すステップと、前記第２の暗号鍵を用いて前記被暗号化暗号鍵を復号化して前記第１の暗号鍵を生成し、生成した前記第１の暗号鍵を記憶するステップと、前記ＲＡＭ領域に記憶された第１の暗号鍵を用いて前記第１の識別情報を暗号化するステップと、前記暗号化した前記第１の識別情報を外部の通信装置に送信するステップと、前記外部の通信装置が記憶する第２の識別情報を含む信号を受信するステップと、受信した前記信号中に含まれる前記第２の識別情報と前記第１の識別情報とを用いて認証処理を行するステップと、を備え、前記ＲＯＭ領域に記憶された前記第１の暗号鍵および前記第１の識別情報は、作動が停止しても情報が保持されることことを特徴とする認証方法。
【請求項４】
前記第２の識別情報と前記第１の識別情報とを用いて行う処理認証は、前記第２の識別情報と前記第１の識別情報とが一致する場合に認証し、一致しない場合は認証しない請求項３記載の認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、自動車等の盗難防止に用いられる車載電子鍵装置および認証方法に関する。
【０００２】
【従来の技術】
従来、電子鍵と車載電子鍵装置を用いて行う盗難防止のための認証方法は、車載電子鍵装置と電子鍵とで識別情報（以下、ＩＤという。）等の所定の情報を無線通信し、受信した信号からＩＤ等を抽出して認証を行い、ＩＤが認証された場合にドアの施解錠を行うものであった（例えば、特許文献１参照。）。その際、車載電子鍵装置と電子鍵とは、車載電子鍵装置毎に異なる共通の暗号鍵を保有し、この暗号鍵を用いて暗号化および復号化を行い、ＩＤの機密性を保持するようにしていた。
【０００３】
ここで、従来の車載電子鍵装置では、車載電子鍵装置毎に異なる暗号鍵を、電子鍵内と車載電子鍵装置内の電気的に書き込み及び消去が可能な不揮発性メモリとに記憶させていた。この不揮発性メモリとして、例えばＥＥＰＲＯＭ等が用いられ、暗号鍵の記憶はもちろん、変更をも行うことができるようにするものであった。
【０００４】

図４に、電子鍵と車載電子鍵装置を用いて行う従来の盗難防止のための認証方法における処理の流れを示すフローチャートを示す。
まず、不揮発性メモリから暗号鍵を読み出し（Ｓ４１０）、車載電子鍵装置が保持する第１のＩＤを暗号鍵により暗号化し（Ｓ４２０）、暗号された第１のＩＤを電子鍵に送信し（Ｓ４３０）、電子鍵によって復号化された第２のＩＤを受信し（Ｓ４４０）、受信した第２のＩＤと上記の第１のＩＤとを比較し、認証を行う（Ｓ４５０）。認証は、２つのＩＤが一致するか否かで行われ、一致した場合に施解錠が行われるものである。
【０００５】
【特許文献１】
特開平８－１７０４５７号公報
【０００６】
【発明が解決しようとする課題】
しかし、このような従来の車載電子鍵装置または認証方法では、内蔵する不揮発性メモリからデータを読み出すことが容易であり、読み出したデータから暗号鍵を推定し、暗号鍵を知ることにより暗号化方式を解読すること容易になり、偽造電子鍵を作成することが可能になるという問題点があった。
【０００７】
本発明はこのような問題を解決するためになされたもので、車載装置から暗号鍵を取得して電子鍵を偽造することを困難にするための車載電子鍵装置および認証方法を提供するものである。
【０００８】
【課題を解決するための手段】
本発明の車載電子鍵装置は、第１の暗号鍵を暗号化して得られる被暗号化暗号鍵を記憶する不揮発性メモリと、前記不揮発性メモリが記憶する前記被暗号化暗号鍵を復号化して前記第１の暗号鍵を生成するために用いる第２の暗号鍵をＲＯＭ領域に記憶した演算処理部とを備え、作動が停止しても前記第２の暗号鍵の情報を保持する記憶領域である構成を有している。
この構成により、被暗号化暗号鍵を復号するための第２の暗号鍵がＲＯＭ領域に記憶されているため、車載装置から暗号鍵を取得して電子鍵を偽造することを困難にすることが可能な車載電子鍵装置および認証方法を実現することができる。
【０００９】
また、本発明の車載電子鍵装置は、外部の通信装置と無線通信するための無線通信インタフェースを備え、前記演算処理部は、さらに認証処理に用いる第１の識別情報をＲＯＭ領域に記憶し、作動時または作動後に前記第２の暗号鍵を用いて前記被暗号化暗号鍵を復号化して前記第１の暗号鍵を生成し、生成した前記第１の暗号鍵をＲＡＭ領域に記憶し、前記ＲＡＭ領域に記憶された第１の暗号鍵を用いて前記第１の識別情報を暗号化し、前記暗号化した前記第１の識別情報を前記無線通信インタフェース経由で前記外部の通信装置に送信し、前記外部の通信装置が記憶する第２の識別情報を含む信号を前記無線通信インタフェース経由で受信し、受信した前記信号中に含まれる前記第２の識別情報と前記第１の識別情報とを用いて認証処理を行い、前記ＲＯＭ領域に記憶された前記第１の識別情報は、作動が停止しても情報が保持される構成を有している。
この構成により、被暗号化暗号鍵を復号するための第２の暗号鍵がＲＯＭ領域に記憶されているため、車載装置から暗号鍵を取得して電子鍵を偽造することを困難にすることが可能であると共に、暗号化した暗号鍵を記憶し、それを復号化して使用する機能または処理を従来の装置に付加するものであるため、新たに付加するハードウェアやソフトウェア等を最小限に抑えることができるため、安価に安全性を飛躍的に向上させることが可能な車載電子鍵装置を実現することができる。
【００１０】
また、本発明の認証方法は、第１の暗号鍵を暗号化して得られる被暗号化暗号鍵を不揮発性メモリから読み出すステップと、前記被暗号化暗号鍵を復号化するために用いる第２の

暗号鍵および第１の識別情報をＲＯＭ領域から読み出すステップと、前記第２の暗号鍵を用いて前記被暗号化暗号鍵を復号化して前記第１の暗号鍵を生成し、生成した前記第１の暗号鍵を記憶するステップと、前記ＲＡＭ領域に記憶された第１の暗号鍵を用いて前記第１の識別情報を暗号化するステップと、前記暗号化した前記第１の識別情報を外部の通信装置に送信するステップと、前記外部の通信装置が記憶する第２の識別情報を含む信号を受信するステップと、受信した前記信号中に含まれる前記第２の識別情報と前記第１の識別情報とを用いて認証処理を行するステップと、を備え、前記ＲＯＭ領域に記憶された前記第１の暗号鍵および前記第１の識別情報は、作動が停止しても情報が保持される構成を有している。

この構成により、被暗号化暗号鍵を復号するための第２の暗号鍵がＲＯＭ領域に記憶されているため、車載装置から暗号鍵を取得して電子鍵を偽造することを困難にすることが可能であると共に、暗号化した暗号鍵を記憶し、それを復号化して使用する機能または処理を従来の装置に付加するものであるため、新たに付加するハードウェアやソフトウェア等を最小限に抑えることができるため、安価に安全性を飛躍的に向上させることが可能な認証方法を実現することができる。

【００１１】

また、本発明の認証方法は、前記第２の識別情報と前記第１の識別情報とを用いて行う処理認証は、前記第２の識別情報と前記第１の識別情報とが一致する場合に認証し、一致しない場合は認証しない構成を有している。

この構成により、暗号化した暗号鍵を記憶し、それを復号化して使用する機能または処理を従来の装置に付加するものであるため、新たに付加するハードウェアやソフトウェア等を最小限に抑えることができるため、安価に安全性を飛躍的に向上させることが可能であると共に、識別情報間の一致を認証の判断基準とするため、簡易なソフトウェアで構成することが可能な認証方法を実現することができる。

【００１２】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を用いて説明する。

（第１の実施の形態）

図１は、本発明の一実施の形態に係る車載電子鍵装置のブロック構成を示す図である。図１において、車載電子鍵装置１００は、暗号化および復号化の処理を含む信号処理を行う演算処理部（以下、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）という。）１１０、暗号鍵を記憶する不揮発性メモリ（ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ－Ｏｎｌｙ Ｍｅｍｏｒｙ）を含む。以下、ＥＥＰＲＯＭともいい、図１および図２にＥＥＰＲＯＭと記す。）１２０、外部の電子鍵２００と無線で通信を行うための無線通信インタフェース１３０、およびＣＰＵ１１０と不揮発性メモリ１２０または無線通信インタフェース１３０とを接続するバス１４０、１５０を含むように構成される。

【００１３】

ＣＰＵ１１０はＲＯＭ領域１１１とＲＡＭ領域１１２を有し、ＣＰＵ１１０のＲＯＭ領域１１１と不揮発性メモリ１２０の記憶領域１２１とには、それぞれ暗号鍵が記憶されている。図２を用いてＣＰＵ１１０のＲＯＭ領域１１１と不揮発性メモリ１２０の記憶領域１２１に記憶されている暗号鍵について説明する。不揮発性メモリ１２０の記憶領域１２１には、第１の暗号鍵を暗号化して得られる情報が記憶されている。以下、第１の暗号鍵を暗号化して得られる情報を被暗号化暗号鍵（図２または図３に暗号鍵１’と記す。）という。

【００１４】

一方、ＣＰＵ１１０のＲＯＭ領域１１１には、被暗号化暗号鍵（図２または図３に暗号鍵１’と記す。）を復号化するために用いられる第２の暗号鍵が記憶されている。暗号化装置１００が作動すると、ＣＰＵ１１０は、不揮発性メモリ１２０に記憶されている被暗号化暗号鍵（図２または図３に暗号鍵１’と記す。）を読み出し、読み出した被暗号化暗号

鍵（図２または図３に暗号鍵１’と記す。）を復号化して第１の暗号鍵を生成し、自己のＲＡＭ領域１１２に記憶する。ＣＰＵ１１０のＲＡＭ領域１１２に記憶された第１の暗号鍵は、ＣＰＵ１１０が作動中は保持され、停止すると消失するものである。

【００１５】

無線通信インタフェース１３０は、車載電子鍵装置１００が外部の電子鍵２００と無線通信し、認証に用いる識別情報（以下、ＩＤという。）を含む情報の送受信を行うようになっている。以下、車載電子鍵装置１００が認証に用いるＩＤを第１のＩＤという。ここで、第１のＩＤは、例えばＣＰＵ１１０のＲＯＭ領域１１１に記憶させておくのでも良く、送信する情報には、暗号化された第１のＩＤが含まれ、受信する情報には電子鍵２００によって復号化されたＩＤが含まれるものとする。バス１４０、１５０は、ＣＰＵ１１０と不揮発性メモリ１２０または無線通信インタフェース１３０とを電気的に接続するものであり、例えばシリアルバスであっても良い。

【００１６】

ここで、電子鍵２００は、上記の第１の暗号鍵を記憶し、暗号化装置１００と無線通信する機能、および無線通信インタフェース１３０経由で送信された情報の復号化を行う機能を有するものとする。そして、電子鍵２００は、無線通信インタフェース１３０経由で送信された情報を復号化して得た情報（以下、第２のＩＤという。）を暗号化装置１００に送信するようになっているものとする。

【００１７】

以下に、本発明の第１の実施の形態に係る車載電子鍵装置の動作について図面を用いて説明する。

図３は、本発明の第１の実施の形態に係る車載電子鍵装置における処理の流れを示すフローチャートである。

まず、被暗号化暗号鍵（図２または図３に暗号鍵１’と記す。）が不揮発性メモリ（ＥＥＰＲＯＭ）１２０からＣＰＵ１１０によって読み出され（Ｓ３１０）、第２の暗号鍵がＣＰＵ１１０のＲＯＭ領域１１１から読み出される（Ｓ３２０）。

【００１８】

次に、ステップＳ３１０で読み出された被暗号化暗号鍵（図２または図３に暗号鍵１’と記す。）がステップＳ３２０で読み出された第２の暗号鍵を用いて復号化されて第１の暗号鍵が生成され、ＣＰＵ１１０のＲＡＭ領域１１２に書き込まれる（Ｓ３３０）。第１の暗号鍵がＣＰＵ１１０のＲＡＭ領域１１２に書き込まれると、認証に用いられるＩＤを第１の暗号鍵を用いて暗号化し（Ｓ３４０）、この暗号化されたＩＤ（以下、第１のＩＤという。）を無線通信インタフェース１３０経由で電子鍵２００に送信する（Ｓ３５０）。

【００１９】

ステップＳ３５０で第１のＩＤが電子鍵２００に送信されたら、電子鍵２００は、第１のＩＤを受信し、受信した第１のＩＤを自己が記憶する暗号鍵を用いて復号化して第２のＩＤを生成し、第２のＩＤを車載電子鍵装置１００に送信するものとする。ここで、車載電子鍵装置１００と電子鍵２００とは、同一の復号化のアルゴリズムを用い、車載電子鍵装置１００によって生成された第１の暗号鍵と電子鍵２００が記憶する暗号鍵とが一致する場合、復号化によって得られた第１のＩＤと第２のＩＤとは一致し、異なる場合、第１のＩＤと第２のＩＤとは一致するようになっている。

【００２０】

ステップＳ３５０で第１のＩＤを電子鍵２００に送信したら、電子鍵２００から第２のＩＤが送信されるのを待ち、送信されたら第２のＩＤを受信する（Ｓ３６０）。そして、暗号化装置１００が保持する第１のＩＤと受信した第２のＩＤとを比較して認証を行う（Ｓ３７０）。認証は、第１のＩＤと第２のＩＤとが一致するか否かを判断することによって行う。言うまでもなく、両者が一致する場合は認証し、そうでない場合は認証しないようになっている。

【００２１】

以上説明したように、本発明の一実施の形態に係る車載電子鍵装置または認証方法は、暗

号化されて不揮発性メモリに記憶された第一の暗号鍵をたとえ不揮発性メモリを取り外して読み出しても、これを復号化しない限り使用することはできないため、暗号鍵を取得して電子鍵を偽造することを困難にすることができる。
また、暗号化した暗号鍵を記憶し、それを復号化して使用する機能または処理を従来の装置に付加するものであるため、新たに付加するハードウェアやソフトウェア等を最小限に抑えることができるため、安価に安全性を飛躍的に向上させることができる。

【００２２】

【発明の効果】

以上説明したように、本発明は、車載装置から暗号鍵を取得して電子鍵を偽造することを困難にするための車載電子鍵装置および認証方法を実現することができる。

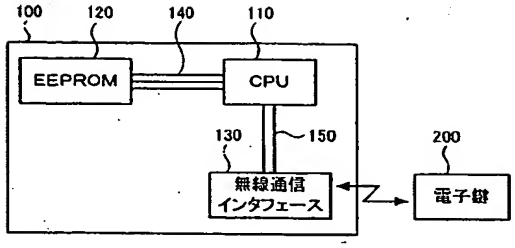
【図面の簡単な説明】

【図１】本発明の一実施の形態に係る車載電子鍵装置のブロック構成を示す図
【図２】本発明の一実施の形態に係る車載電子鍵装置において記憶される暗号鍵の記憶場所について説明するための図
【図３】本発明の一実施の形態に係る認証方法における処理の流れを示すフローチャート
【図４】従来の認証方法における処理の流れを示すフローチャート

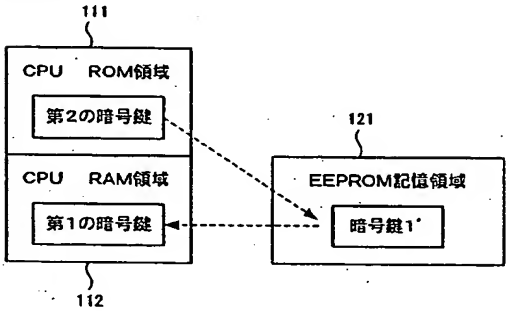
【符号の説明】

１００　車載電子鍵装置
１１０　演算処理部（ＣＰＵ）
１１１　ＣＰＵのＲＯＭ領域１１１
１１２　ＣＰＵのＲＡＭ領域１１２
１２０　不揮発性メモリ
１２１　不揮発性メモリの記憶領域１２１
１３０　無線通信インタフェース
１４０、１５０　バス
２００　電子鍵

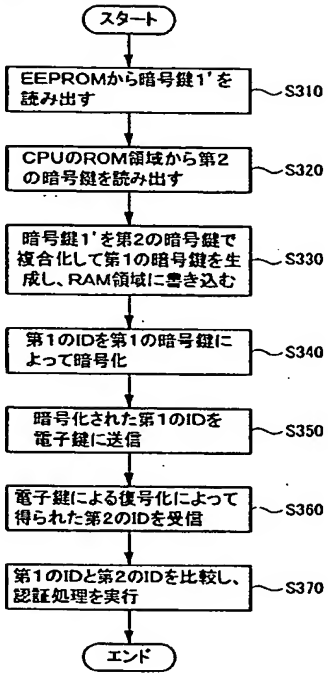
【図１】


100
120
140
110
EEPROM
CPU
130
150
200
無線通信
インタフェース
電子鍵

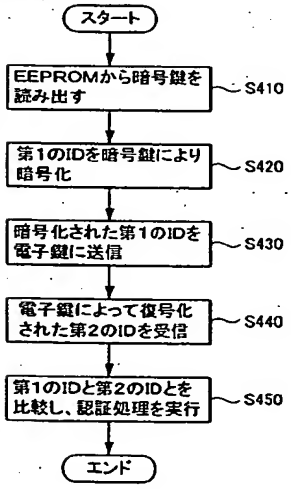
【図２】


111
CPU ROM領域
第2の暗号鍵
121
CPU RAM領域
EEPROM記憶領域
第1の暗号鍵
暗号鍵1'
112

【図３】


スタート
EEPROMから暗号鍵1'を読み出す
S310
CPUのROM領域から第2の暗号鍵を読み出す
S320
暗号鍵1'を第2の暗号鍵で複合化して第1の暗号鍵を生成し、RAM領域に書き込む
S330
第1のIDを第1の暗号鍵によって暗号化
S340
暗号化された第1のIDを電子鍵に送信
S350
電子鍵による復号化によって得られた第2のIDを受信
S360
第1のIDと第2のIDを比較し、認証処理を実行
S370
エンド

【図４】


スタート
EEPROMから暗号鍵を読み出す
S410
第1のIDを暗号鍵により暗号化
S420
暗号化された第1のIDを電子鍵に送信
S430
電子鍵によって復号化された第2のIDを受信
S440
第1のIDと第2のIDとを比較し、認証処理を実行
S450
エンド

フロントページの続き

(51) Int. Cl.[7]	F I	テーマコード (参考)
H04L 9/32	H04L 9/00 673C	